BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G07F 7/12, H04M 17/00

A2

(11) International Publication Number: WO 96/24913

(43) International Publication Date: 15 August 1996 (15.08.96)

(21) International Application Number: PCT/GB96/00269

(22) International Filing Date: 6 February 1996 (06.02.96)

(30) Priority Data:
08/386,146 8 February 1995 (08.02.95) US

(71) Applicant: NEXUS 1994 LIMITED [GB/GB]; 7-10 Chandos Street, London W1M 9DE (GB).

(72) Inventors: YOKEV, Hanoch; 8 Hazanchanim Avenue, 52341 Ramat-Gan (IL). MEIMAN, Yehouda; 31 Ben Eliezer Street, 75299 Rishon Letzian (IL).

(74) Agents: BERESFORD, Keith, Denis, Lewis et al.; Beresford & Co., 2-5 Warwick Court, High Holborn, London WC1R 5DJ (GB).

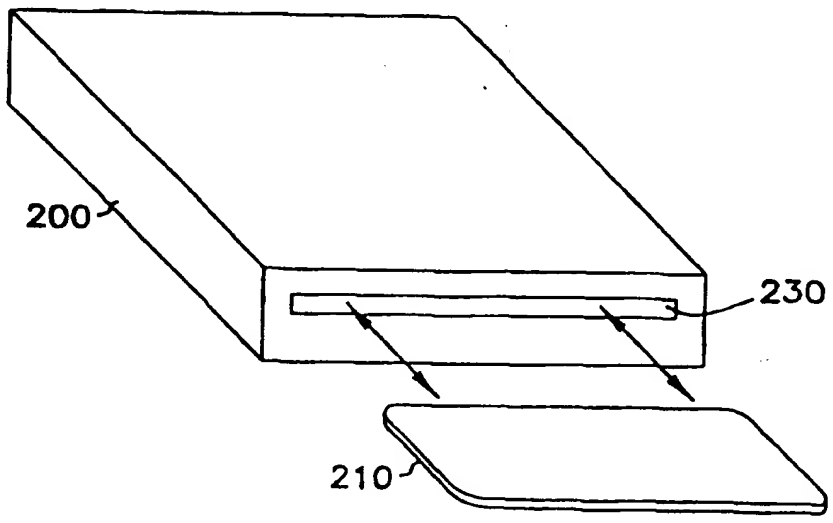
(81) Designated States: JP, KR, SG, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: TWO-WAY MESSAGING NETWORK USING DEBIT CARDS

(57) Abstract

A two-way messaging network is described which allows a user of a remote communicator to use pre-paid debit cards to authorize message communication. The debit card consists of a storage medium for storing a pre-paid authorization value and anti-counterfeit protection. The remote communicator has the ability to communicate with a base station and debit the authorization value according to the amount of communication time used. The remote communicator also has anti-counterfeiting protection which is used in combination with the debit card to deter unauthorized communications using counterfeit components.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia
AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

TWO-WAY MESSAGING NETWORK USING DEBIT CARDS

FIELD OF THE INVENTION

The present invention relates generally to communication systems and in particular the present invention relates to two-way messaging. More particularly, the present invention relates to protecting against unauthorized communication using counterfeit components of a two-way messaging network.

BACKGROUND OF THE INVENTION

Current two-way communication systems such as cellular telephones rely on a billing system to charge customers for individual usage. In a cellular telephone system, the customer is typically charged a monthly fee and charged for the length of communication time used by the user. The service provider, therefore, must compute the charges for each user and operate an often expensive billing and collection system.

To avoid billing for the limited use of apparatuses such as photo copy machines and pay phones, pre-paid systems are used. These pre-paid systems include the purchase of a debit card which stores a pre-paid authorization value which is debited according to the amount of usage of the apparatus. While the use of debit cards reduces the burden of billing, debit cards are susceptible to being counterfeited.

Remote communicators such as cellular phones are also susceptible to the use of counterfeit components. Unlike public pay-phones or photo copy machines, the mobile nature of a cellular phone allows a counterfeiter to substitute counterfeit electrical components for valid components in a communicator to bypass the payment system or charge the usage to another user. Counterfeiting the electrical components of a communicator is possible if the counterfeiter identifies the protocol used by the communication network to compute and bill for usage.

For the reasons stated above, and for other reasons stated below which will become apparent to those skilled in the art upon reading and

understanding the present specification, there is a need in the art for a credit system to pre-authorize communication from a remote communicator which protects against the use and development of counterfeit components.

SUMMARY OF THE INVENTION

The above mentioned problems with credit systems in messaging networks and other problems are addressed by the present invention and which will be understood by reading and studying the following specification. The present invention is a method of authorizing transmissions from a plurality of remote communicators to a base station. The method comprising the steps of, reading a coded protection word stored on a storage medium of a debit card with one of the plurality of remote communicators, decoding the coded protection word with the remote communicator and generating a key word based on the decoded protection word, communicating the key word to the debit card, and evaluating the key word with the debit card and authorizing the remote communicator to transmit to the base station based on the key word and an authorization value stored on the storage medium. The method can further include the step of providing the debit card with a custom protection word and a custom key word for use by one of the plurality of remote communicators.

Another embodiment provides an alternate method of authorizing transmissions from a plurality of remote communicators to a base station. The alternate method comprising the steps of, reading a coded protection word stored on a storage medium of a debit card with one of the plurality of remote communicators, transmitting the coded protection word to the base station using the remote communicator, comparing the received coded protection word with a master list of valid coded protection words stored at the base station, transmitting a validation signal to the remote communicator indicating if the coded protection word is valid, and authorizing the remote communicator to transmit to the base station based on the validation signal and an authorization value stored on the storage medium of the debit card. The storage medium can be a magnetic strip.

Still another embodiment provides another method of authorizing transmissions from a plurality of remote communicators to a base station. This method comprising the steps of, generating a pseudo random code word using one of the plurality of remote communicators, communicating the pseudo random code word to a debit card comprising a storage medium containing an authorization value and a decoding algorithm, decoding the pseudo random code word using the decoding algorithm and communicating the decoded pseudo random code word to the remote communicator, and reading the authorization value from the storage medium if the decoded pseudo random code word is correct.

BRIEF DESCRIPTION OF THE DRAWINGS

In the drawings, where like numerals refer to like components throughout the several views,

Figure 1 is an overview of the infrastructure of the multi-path resistant frequency-hopped spread spectrum mobile location system;

Figure 2 describes the synchronization and message format of the outgoing paging signals from the base stations;

Figure 3 describes the format of the frequency-hopped spread spectrum signal transmitted by the remote mobile units;

Figure 4 is a remote communicator and a debit card of the present invention;

Figure 5 is a block diagram of the remote communicator and a debit card of Figure 4;

Figure 6 is a flow chart of the operation of the remote communicator and a debit card of Figure 4;

Figure 7 is an alternate block diagram of the remote communicator and a debit card of Figure 4;

Figure 8 is another alternate block diagram of the remote communicator and a debit card of Figure 4; and

Figure 9 is an alternate flow chart of the operation of the remote communicator and a debit card of Figure 4.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

In the following detailed description of the preferred embodiment, reference is made to the accompanying drawings which form a part hereof, and in which is shown by way of illustration specific preferred embodiments in which the inventions may be practiced. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, and it is to be understood that other embodiments may be utilized and that structural, logical and electrical changes may be made without departing from the scope of the present inventions. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present inventions is defined by the appended claims.

The present invention is directed to granting financial authorization for communication time to communicate messages from remote mobile units. The present invention allows for granting financial authorization for communication to users of remote mobile units who may have questionable credit worthiness, such as children. The remote mobile units may be located in motor vehicles, located on the person of people, carried within containers or packages, or any number or variety of mobile carriers. The communication system comprises one or more base stations which transmit signals to the remote mobile units and receive signals from the remote mobile units. The base stations may send messages and information to the remote mobile units, or the base stations may simply send alert or interrogation commands to activate the remote mobile units. Thus the remote mobile units may be activated locally (for example by the wearer or vehicle) or remotely by the base station. The remote mobile units may be used by a person as a reverse pager, as an emergency locator or as a communication device. The remote mobile units may also be used as part of a vehicle to locate the vehicle if stolen, in an accident, for vehicle tracking or as an integral communication device.

The remote mobile units receive messages as a standard paging device over licensed airwaves using a standard paging infrastructure. The remote mobile units, when activated, transmit low-power (less than one watt),

frequency-hopped, spread-spectrum communication signals. The transmitted signals from the remote mobile units are received by the base stations. The remote units accept special debit cards for authorizing communication time from the remote unit to the base. A protection system is used to prevent the modification or impersonation of either the remote unit or the debit card. Following a detailed description of the two-way message system, the debit card and protection system are described in detail.

Two-Way Messaging System Overview

In the preferred embodiment of the present invention, the transmitters and base stations of the present invention are as described in U.S. Patent Number 5430759 entitled "LOW-POWER FREQUENCY-HOPPED SPREAD SPECTRUM ACKNOWLEDGMENT PAGING SYSTEM". The infrastructure of this acknowledgement paging systems serves as the basis of the present system and the reverse pagers of this acknowledgement pager system operate identically in the present system.

Figure 1 depicts the major components of the two-way paging system in the aforementioned U.S. Patent Number 5430759 entitled "LOW-POWER FREQUENCY-HOPPED SPREAD SPECTRUM ACKNOWLEDGMENT PAGING SYSTEM". In the preferred embodiment of the present invention, all of the components of the existing paging system of Figure 1 are used. The reverse paging terminal 110 at the central site operates to provide synchronization and messaging information through the paging terminal 116 to the reverse pagers 100 (also known as remote mobile units 100) via direct links to the base stations BS_1, BS_2 and BS_3 through ground based radio links (not shown) or through a satellite uplink/downlink using a geostationary satellite (not shown). The base stations BS_1, BS_2 and BS_3 include transmit and receive towers 113a, 113b and 113c, respectively and base station terminals 201a, 201b and 201c, respectively. Terminals 201a-201c are required for producing the accurate synchronization information needed to be transmitted to the remote mobile units and for local processing of the received messages. This synchronization

information is used to coordinate the frequency hopping transmissions and to coordinate the response of messaging from the plurality remote mobile units 100 so as to minimize collisions within groups of remote mobile units and eliminate collisions between groups of remote mobile units.

Base to Remote Synchronization

Standard paging messages sent from the base stations BS_1, BS_2 and BS_3 to the plurality of remote mobile units 100 are, in the preferred embodiment, sent as digital data encoded in the POCSAG paging standard. These messages may be used to interrogate the remote mobile units to activate the remote mobile unit to allow the base stations to begin the location process. Typically the paging channel has a center frequency of 143.160 MHz, with an NRZ FSK data rate of 512 bps or 1200 bps. Other bit rates such as 2400 baud (bps) are also feasible. Figure 2 describes the POCSAG paging communications protocol as modified for use by the preferred embodiments of the present invention. In the top line of Figure 2, a greatly compressed time line of digital data transmitted according to the POCSAG protocol is shown. Batches of messages are transmitted in groups as shown in the details in the subsequent lines below the top line of Figure 2. In the second line of Figure 2, a 1.0625 second interval (for 512 baud) is shown in which 544 bits are transmitted as a single batch. The batch is preceded by a synchronization code word SC as shown in the third line of Figure 2.

The synchronization code word within each batch is followed by eight frames of digital data. Each frame is divided into two portions, an address portion and a message portion. The address code word of the message of frame 2 of Figure 2 is shown in line 4 while the message code word of the second half of frame 2 is shown in line 5. The address code word is preceded by a digital zero followed by 18 address bits, two function bits and 10 check bits. The address code word is followed by an even parity bit. The message code word portion of the frame is preceded by a digital one followed by 20 message bits which are followed by 10 check bits and a single even parity bit. Thus each frame is comprised of 64 bits divided into two 32 bit sections.

Synchronization of the base station terminal 200 and the remote mobile units 100 is necessary to ensure the units 100 are transmitting at the same time that the base stations are listening. Synchronization is also necessary to coordinate the division of the large number of remote mobile units into groups so that members of one group use different frequency hopping patterns from members of other groups. Synchronization of the remote mobile units 100 is accomplished by inserting a special frame into the POCSAG data which is used to synchronize the units.

The purpose of the synchronization between the reverse paging terminal 110 and the remote mobile units 100 is to determine where along the pseudo random noise code the frequency hops are to be followed and to determine the exact times for transmitting frequencies from within any of the hops. This also enables the dynamic changing of a remote mobile units group membership such that if one group is experiencing a large number of collisions due to simultaneous transmissions, the reverse paging terminal 110 may re-allocate some of the remote mobile units within that group to new groups to minimize collisions.

Referring once again to Figure 2, eight frames of information are transmitted in each burst using the POCSAG format. Remote mobile units 100 may be assigned to a specific frame within the transmission so that the remote mobile units, once recognizing the synchronization code word, can scan a specific frame for that remote mobile unit's address. Once the address is found, the remote mobile unit can determine any group changes that may be required to re-allocate that remote mobile unit to a different group. In addition, the POCSAG format is used to transmit a fine time synchronization code. The fine synchronization code is a transmission of a time pulse at an exact time synchronized to a GPS (Global Positioning System) clock to synchronize all the remote mobile units 100 for time of transmission. For example, periodically during the day the reverse paging terminal will send a synchronization code within the POCSAG code word which is sent at a very precise time. In order to ensure that a precise time pulse is sent, the reverse paging terminal 110 receives accurate time information using a GPS antenna

to receive accurate time of day information. The time used to send the synchronization pulse is when the day clock reaches exactly some multiple of 0.9 seconds in the preferred embodiment. In this synchronization information, 20 bits of information are transmitted to give the accurate time of day information.

In each of the remote mobile units 100, the microprocessor compares this accurate time pulse which will indicate the exact time of day and compare it to its own day clock. The clock within each microprocessor is accurate down to a few milliseconds, but the time at which the synchronization pulse occurs should have a resolution much finer than that such as down to 0.1 milliseconds for time of day. In this fashion, each of the microprocessors in each of the remote reverse paging devices can periodically realign its day clock to know within a millisecond the exact time. Each microprocessor does not actually realign its clock but changes a clock offset within memory so that it understands how far off its own internal clock is and can make the adjustment when using that clock to determine when to start transmitting information.

The synchronization pulse is only transmitted every few minutes. However, the resolution of the start of the message indicating the synchronization pulse is very accurate, it being transmitted at 0.090000 seconds GPS time after a fixed time of day, such as 12:00 GMT. This GPS time is accurate to at least within 100 nanoseconds.

An overview of the transmission format of the remote mobile unit is shown in Figure 3. The actual transmission of information from the remote mobile units 100 is done using Differential Bi-Phase Shift Keying (DBPSK) modulation on a frequency hopped carrier of less than one watt. The transmission of information from the remote mobile units 100 on the frequency hopped carrier may also be done using Frequency Shift Keying (FSK) modulation. Typically a single transmission consists of 53 hops or 53 changed frequencies selected from a list of narrow band frequencies. The frequency selection is based on a pseudo-random noise code list pointing to the frequency selection list. The synchronization information tells the remote

mobile unit 100 where along the pseudo random noise code it should be synchronized for transmission of its message and tells exactly the time of day so that the remote mobile unit 100 knows exactly when to start transmitting the specific frequency that the base stations BS_1, BS_2 and BS_3, labeled 113a, 113b, and 113c, respectively, are looking for that frequency at the same time.

In operation, 200 frequencies are used by the remote mobile unit 100 and the base stations and internally stored in a list numbered F1 through F200. For a specific message, 53 frequencies will be used to transmit the entire message. These 53 frequencies are selected based on a 1,000 member pseudo-random noise code.

The use of the accurate synchronization signal periodically broadcast via the outbound paging signal enables the remote mobile units to use lower accuracy components thus reducing the manufacturing cost of remote mobile units. For example, high accuracy crystals to track the time of day within the microprocessor are available with an accuracy of three parts per million. Thus, a time drift of approximately three micro seconds per second or 180 microseconds in a minute is the known drift. There are also time inaccuracies which are introduced due to the variable path length between the paging tower and the remote mobile unit. By employing crystals which are cheaper and have an accuracy of the order 50 parts per million, the amount of time-of-day drift normally wouldn't be tolerable. However, by using the synchronization information transmitted on a regular basis from the reverse paging terminal, the microprocessor can continually correct its own internal day clock so that accurate time of day measurements are always maintained. The microprocessor estimates the momentary inaccuracy of the crystal by tracking the drift across several synchronization transmissions and dynamically adjusts for the frequency drift of the crystal and the offset using internal offset registers for accurate time of day information.

Counters are employed within each microprocessor of the reverse paging units to compensate for the offset of the frequency based on the synchronization time information. There are generally two major factors

which affect the drift in a crystal: temperature and acceleration. Most of the drift is due to temperature, and the remaining drift components are negligible. The frequency drift in a crystal due to temperature is very slow, on the order of 50 Hz over 10 seconds. During a single day the temperature can change by 20 or 30 degrees fahrenheit, requiring a time update from the GPS clock approximately every five minutes.

Remote Mobile Unit Transmission Format

The signal sent from the remote mobile unit 100 to the base stations is a spread-spectrum, frequency-hopped transmission using differential bi-phase shift keying (DBPSK) modulation on the frequency-hopped carrier to transmit digital information. The transmission of information from the remote mobile units 100 on the frequency hopped carrier may also be done using Frequency Shift Keying (FSK) modulation. The frequency hops are relatively slow, the frequencies transmitted are very narrow and the transmission power is extremely small. The maximum peak output power of transmission from remote mobile unit 100 is limited to less than one Watt to allow use of the 902-928 MHz ISM band in the United States without the need for licensing the remote units as allowed by FCC regulations defined in 47 C.F.R. §15.247. Those skilled in the art will readily recognize that other frequency bands and transmissions power levels may be employed depending upon FCC licensing requirements or other frequency licensing requirements of other nationalities.

The use of an accurate crystal to control each frequency of transmission is required within each remote mobile unit 100. For example, high accuracy crystals to transmit the narrow bandwidth frequencies used for the frequency hopped transmissions are available with an accuracy of three parts per million. At 900 MHz, a 3 ppm drift would place a single frequency somewhere within a 2.7 KHz band. To tolerate frequency drift due to aging and temperature, each individual frequency of the frequency hopped signal is allocated to a 7.5 KHz band or channel, even though the actual frequency is on the order of 200 Hz wide skirt within this 7.5 KHz allocated bandwidth. Those skilled in the art will readily recognize that by using alternate components, the frequency channels (individual frequency of the frequency

hopped signals) of 7.5 KHz allocated bandwidth may be wider or more narrow depending upon the overall allocated bandwidth for the system. For example, 1 KHz or less bands may alternatively be allocated per channel.

Tests on this system have shown that by processing the received signals at the base stations entirely in the digital domain using the combination of unique Fast Fourier Transform algorithms to locate and retrieve the frequency hops and by using a combination of unique confidence algorithms with a plurality of error correction codes, the receiving base station is able to pull the response information from a very low power signal from a distance of up to 45 kilometers (28 miles) in a flat terrain. In a rather noisy urban environment, a range of 24 kilometers (15 miles) is the norm. The information within the signals is accurately decoded even in severe multipath and noise conditions.

As shown in Table 1, the remote mobile unit message format consists of a preamble and the message body spanning a total of 53 frequency hops. Those skilled in the art will readily recognize that longer messages may be transmitted using the preferred embodiment of the present invention, and the messages format described here is illustrative but not limiting. Much longer message hops to transfer more digital data is also implemented but not described here. Of course, those skilled in the art will readily recognize that shorter messages than those described below are equally possible for the preferred embodiments of the present invention. The message length and number of transmission hops are a matter of design choice.

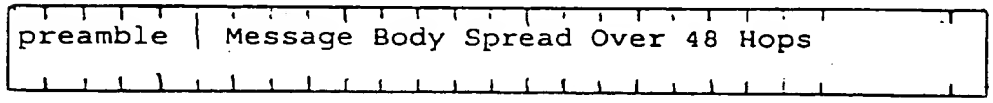
The message preamble consists of a predefined code of ones and zeros to get the attention of the base unit receiver to pull the message out of the noise. The preamble consists of 165 bits transmitted across 5 hops, that is, transmitted using DBPSK (Differential Bi-Phase Shift Keying) or Frequency Shift Keying (FSK) on five different frequencies selected from the frequency list with the specific frequencies selected based on the PN (Pseudo-random Noise) Code list stored within the remote mobile unit. The sequence location within the PN code that the remote mobile unit will begin to follow is based on the synchronized time of day. Within a single hop (a single carrier

frequency), the carrier phase is modulated 33 times to encode the predefined one-zero pattern of the preamble.

The message body follows the preamble and consists of three groups of data. Each group consists of 30 actual data bits so that the entire message is, in the preferred embodiment of the present invention, 90 total data bits (although other bit length messages may be chosen). The actual data encoded within these 90 bits is described above and may be in any convenient coded format. Those skilled in the art will readily recognize that a wide variety of message formats and encoding of the data bits may be used without departing from the scope of the present invention. The encoding described here, however, has been proven effective in retrieving the data bits buried in background noise with a high degree of accuracy and a low actual error rate.

TABLE 1: Remote Mobile Unit Message Format

Preamble is 165 bits (33 bits x 5 hops)
Message is 48 * 33 transmitted bits
(Message is 90 bits actual data)
[] = One Frequency Hop



Outer Message Coding

Each of the three groups of message data (30 bits each) are BCH encoded using a standard 30,63 BCH code and with a single parity bit added to form a 64-bit word. This encoding decreases the error rate from 10^{-2} to 10^{-5}. This encoding, documented and understood by those skilled in the art, can correct up to 6 errors or detect up to 13 errors. Detection of corruption of a data word that cannot be reconstructed will cause the base to request a second transmission of the acknowledgement message.

Inner Coding and Interleaving

The inner coding of the message will protect the integrity of the message with an error rate as high as 25%. Each block of 64 bits of data (corresponding to a groups of 30 bits and earlier encoded by a standard 30,63 BCH code) is split into two sub-blocks of 32 bits (sub-blocks A and B of Table 2), and a reference bit is added to each sub-block to assist the differential encoding to provide a reference bit to the DBPSK or FSK decoder. The 33 bit sub-blocks are transmitted over one frequency hop each and are replicated 8 times so that the 64-bit block traverses 16 frequency hops. In transmission, the 33 bit sub-blocks are interleaved to further reduce loss of data, as shown in Table 3, where sub-blocks A and B of Table 2 correspond to the first group of 30 bits, sub-blocks C and D, correspond to the second group of 30 bits, etc. The total message is 53 hops where each hop is 180 msec in length making the duration of a single message 9.54 seconds.

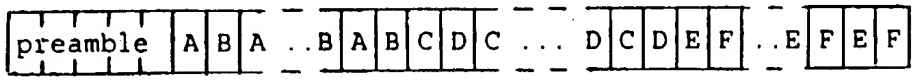
TABLE 2: Interleaving Format for Sub-block

A = 1 reference bit and 32 data bits = 33 bits
B = 1 reference bit and 32 data bits = 33 bits
☐ = One Frequency Hop

TABLE 3: Inner Coding and Interleaving of Sub-blocks

A = first 33 bits of 1st block
B = second 33 bits of 1st block
C = first 33 bits of 2nd block
D = second 33 bits of 2nd block
E = first 33 bits of 3rd block
F = second 33 bits of 3rd block

[] = One Frequency Hop



Those skilled in the art will readily recognize that a wide variety of data interleaving may be utilized to effect better error tolerance and may be substituted for the interleaving described here. Such alternate substitute interleaving means are CIRC (Cross Interleaved Reed Solomon Code) used in CD (Compact Disc) recording media operating either at the block level or at the bit level.

Single Hop Format

The acknowledgment signals are transmitted by the remote mobile units 100 in a 1.5 MHz band selected from within the 902-928 MHz spectrum. The 1.5 Mhz band is divided into 7.5 KHz channels to provide 200 channels available in which the frequency hops can occur. Thus, each frequency hop is a channel 7.5 KHz wide in which a carrier frequency is transmitted. For example, channel one will have a frequency F1 at 902.00375 MHz +/- 3.75 KHz, channel two will have its center carrier frequency at 902.01025 MHz +/- 3.75 KHz, etc.

Each transmit frequency of each hop will thus be centered at the approximate mid-point of the assigned channel band; however, due to inaccuracies in the remote mobile unit circuits and reference crystals, the actual transmit frequencies will vary between units. If high quality crystals are used to accurately produce the required frequencies, very little drift off the center frequency will result. In the preferred embodiment of the present invention, low cost crystals are purposely employed to keep the per-unit manufacturing costs down. This will allow for a lower-cost product sold to the user which will increase market penetration. Thus, reference crystals are preferred which have a frequency accuracy of 3 ppm such that at 900 MHz, the statistical drift would be approximately 2700 Hz. The crystals center frequency within its nominal accuracy also drifts due to aging and temperature variations, but this drift is slow compared to the transmission times so the drift during a single transmission due to these latter variants is unimportant.

A single frequency hop is shown in Table 4. The 15 millisecond guard time preceding each hop is primarily a settling time for the oscillator

circuits of the remote mobile units to allow the internal oscillator circuit to lock onto the new frequency between hops. Each hop is transmitted at a single frequency in which the phase of the carrier is either at 0 degrees phase or 180 degrees phase in reference to the phase of the reference bit immediately following the quiet or guard time. Thus the first bit is a phase reference bit followed by 32 data bits exhibiting either zero phase shift or 180 degree phase shift to encode the data bits as DBPSK (Differential Bi-Phase Shift Keying). In an alternative implementation, each frequency hop may be modulated using Frequency Shift Keying (FSK) in which two frequencies are used to transmit data bits. One hop frequency may indicate a logical one while a second hop frequency may indicate a logical zero. The frequency shift is minor and the frequency differential is contained within a single hop channel.

Each bit of DBPSK or FSK is a transmission of 5 milliseconds of the hop carrier frequency either in phase with the reference bit transmission or 180 degrees out of phase.

TABLE 4: Single Frequency Hop Format

Guard time (quiet) = 15 ms
Single Bit = 5 ms of carrier DBPSK / FSK
33 Bits plus guard time = 180 ms

15ms Guard Time	5ms Ref Bit	5ms 1st Bit	5ms 2nd Bit	5ms 3rd Bit		5ms 31st Bit	5ms 32nd Bit

Frequency Hopping Sequence

All of the remote mobile units in the market serviced by the reverse paging terminal for message or location finding use the same pseudo random noise code to determine the frequency hops. The pseudo random noise code is a digital code of 1,000 unique numbers. In the preferred embodiment of the present invention, the pseudo random noise code is stored in memory of

each of the remote mobile units. Those skilled in the art will readily recognize, however, that a linear feedback shift register could be used to generate the pseudo random noise code on a real-time basis instead of using a look-up table which is presently in the preferred embodiment.

The PN (pseudo-random noise) code list is stored in memory and maps to a frequency list. In the preferred embodiment of the present invention, the PN code list has 1,000 entries which repeat as a sequence. The control means of the reverse paging units continuously maintain a count of the proper location within this list. As described below, the time of day for all remote mobile units in the market served by the base terminal are periodically synchronized to ensure acknowledgment messages are synchronized to transmit the hop frequency at the proper time and to synchronize the location within the PN code list that each remote mobile unit will use to transmit.

The 1,000 member PN code list maps to a 200 member frequency list. In order to allow a large number of remote mobile units to simultaneously operate in the same geographic market, the remote mobile units are divided into groups and the groups are assigned different sequence segment locations in the same 1,000 member PN list. Thus a remote mobile unit from group one will begin transmitting a hop at a frequency determined from a first location with the PN code, while a remote mobile unit from group two may begin transmitting a hop at a frequency determined from a second location in the PN code. The remote mobile units from group one and group two will complete their respective acknowledgement messages in 53 hops. Preferably, the sequence of the PN code used to determine the frequencies of the 53 hops for the remote mobile unit of the first group will not overlap the sequence of the PN code used to determine the frequencies of the 53 hops for the remote mobile unit of the second group. More preferable, the frequencies chosen based on the non-overlapping segments of the PN code list are orthogonal such that the same frequency is never used by two remote mobile units belonging to different groups.

In the preferred implementation, the 1,000 member PN code list is divided into 160 hopping sequences. The remote paging units are divided into

40 groups with the members of each group synchronized to track the same location in the PN code list. The microcontroller of each remote mobile unit, regardless of its group membership, continuously runs through the repeating PN code sequence to stay in synchronization with the base unit and all other remote mobile units. Each group of remote mobile units is further divided into four subgroups such that the remote mobile units within each subgroup are assigned one sequence within the PN code list. Although the 53 hop sequence needed for each acknowledgement transmission may overlap the 53 hop sequence used by a remote mobile unit in another subgroup, the transmission sequences of a remote mobile unit of one group is chosen to not overlap the 53 hop sequence used by a remote mobile unit in another group.

Base Station Design

As described in US Patent number 5430759, the analysis and decoding of the signals received by the base stations from the remote mobile units is done almost entirely in the digital domain. The carrier frequencies of the frequency hops are down-converted to a lower frequency in each base station and are then digitally sampled. The digital samples are then processed to locate the phase information of interest for direction finding and message decoding. Each base station is constructed with a plurality of digital signal processor pipelines which enable simultaneous message decoding and direction finding of a plurality of simultaneously transmitting remote mobile units.

Debit Card System

In the pre-paid debit card system of the embodiment of the present invention the user of a remote communicator 200 or paging unit purchases a debit card 210 to allow the user to pre-pay for the two-way messaging service, as shown in Figure 4. The debit card to be used with a remote communicator is preferably the approximate size and shape of a common credit card. The debit card stores an indication of the amount of pre-paid communication time available to a user. The debit card provides financial authorization for communication, thereby enabling communication with users having questionable credit such as children. It can be seen that there is monetary value associated with the card

which provides an incentive to counterfeit the debit card for resale or personal use. Therefore, protection must be provided to deter the manufacture of counterfeit cards or other components critical to the operation of the pre-paid debit card system.

Referring to Figure 5, the debit card 210 has a storage medium 220 thereon for storing an authorization value corresponding to the pre-paid value of the debit card. The authorization value is preferably an indicator indicating to the remote communicator the amount of authorized time available for transmitting messages to the base unit.

The communicator 200 preferably has a physical slot 230 or groove therein for receiving the debit card 210 and is capable of reading from and writing to the storage medium of the debit card. To protect against the unauthorized manufacturing or counterfeiting of either the debit card or the remote communicator, anti-counterfeiting protection is incorporated in both the communicator and the debit card. For example, a counterfeiter may attempt to produce a counterfeit component by connecting a logic analyzer to the communication lines 242 between the card and the communicator. The communicator would be activated and the logic analyzer records all data transferred between the communicator and the debit card. Based on the recorded data a counterfeit component might be developed.

In the preferred embodiment, referring to Figure 5, the communication system is protected against counterfeiters by using a coded protection word stored on the debit card 210 and a unique protocol between the remote communicator 200 and debit card. The storage medium is not directly readable, but can only be read after following the following sequence. When a new debit card is inserted into a remote communicator, the remote communicator reads the coded protection word from the storage medium of the debit card. A decoder circuit 240 of the remote communicator then decodes the coded protection word using a unique algorithm and generates a key word based on both the algorithm and the coded protection word. The remote communicator then provides the key word to the debit card via the communication lines 242. In turn, the anti-counterfeit protection on the debit

card, which preferably comprises a microprocessor 244, evaluates the key word provided from the remote communicator. If the remote communicator has used the correct algorithm, the debit card authorizes the remote communicator to read and modify the authorization value stored in the storage medium 220. It will be understood by one skilled in the art that the protection word can be varied from debit card to debit card such that decoding the unique algorithm is difficult for a counterfeiter. Further, a variety of key words can be used to allow for the periodic changing of the algorithm.

As the remote communicator 200 transmits to the base unit using transmitter 246, the authorization value stored on the debit card 210 is updated or automatically debited to reflect the amount of pre-paid transmission time used. The debit card is preferably updated by physically blowing a portion of programmable read only memory (EPROM) provided as the storage medium 220 on the debit card. The debit card will only accept a pre-determined number of incorrect key words before inactivating itself. The debit card, therefore, must be used by a user with a remote communicator containing a valid algorithm.

Referring to Figure 6, a flow chart illustrates the method of authorizing transmission from a remote communicator 200 to a base station using the preferred embodiment. After the remote communicator reads the protection word from the debit card 210, it computes and outputs the key word to the debit card. If the remote communicator outputs the correct key word, the communicator can read and update the content of the authorization value. The debit card will shut down if the incorrect key word is output four times, by way of example, but not by limitation. After the debit card has recognized the correct key word from the remote communicator, the user of the remote communicator can provide the debit card with an optional updated custom protection word and a corresponding key word for continued use by that customer's particular remote communicator. This option provides an additional layer of protection, such that if the user were to lose his/her debit card, another user could not use the debit card in another remote communicator and transmit to a base unit using the remaining pre-paid

authorized transmission time on the debit card. This option also deters the theft of valid debit cards.

The preferred embodiment provides a debit card which protects against reading valid debit cards in an effort to understand the protection and counterfeit the cards. Referring to Figure 7, in an alternate embodiment the remote communicator 200 provides additional protection against counterfeit debit cards or electronics that emulate the output of the debit card. In the alternate embodiment, the debit cards have a storage medium 220 with a unique coded protection word stored thereon. When a new debit card is inserted into a remote communicator the remote communicator reads the protection word and transmits that word to the base unit via transmitter 246. The base unit then compares the received protection word against a master database which contains a list of all valid protection codes currently in use on issued debit cards. If the debit card's protection code matches a valid protection code, the base unit notifies a receiver 250 of the remote communicator with a validation signal. Similarly, if the protection code is invalid the remote communicator is notified with an invalid signal. If the debit card is valid, the remote communicator is authorized to transmit messages to the base unit and debit the authorization value in accordance with the length the communication. An optional feature for this embodiment allows the base unit to transmit a new validation code to the remote communicator such that the remote communicator can update the protection word on the debit card. This option allows the user of the remote communicator to use a semi-custom protection word similar to that available in the preferred embodiment to deter theft. The base unit then deletes the original protection word from the database, thereby reducing the amount of protection words stored therein. The storage medium of the debit card is preferably a magnetic strip for storing the authorization value and the coded protection word.

In a second alternate embodiment directed to protect the debit card system, a debit card 210 having a microprocessor 252 is used, see Figure 8. The debit card has a unique decoding algorithm stored in the microprocessor.

In this embodiment, the remote communicator 200 provides the debit card a code word that is generated pseudo-randomly by a code generator 254 to be a "random code." The debit card decodes the random code using the unique decoding algorithm and generates a decoded random code using the micro processor 252. This decoded random code is provided to the remote communicator and the remote communicator evaluates the decoded signal to verify that the debit card contains the correct algorithm. If the use of the correct algorithm is detected the remote communicator reads and writes to the storage medium 220 of the debit card. If the correct algorithm is not detected the debit card is ignored.

It will be understood by one skilled in the art that any or all of the embodiments can be combined to provide multiple protection against counterfeit debit cards and communication devices. Figure 9 illustrates the method of authorizing transmissions from the remote communicator 200 to a base unit using a combination of the preferred and second alternate embodiments. As illustrated, after the remote communicator generates and outputs a random code word, the debit card returns a decoded random word. If the decoded word is a correct match the remote communicator reads a protection word stored on the debit card. The remote communicator generates a key word based on the protection word and outputs the key word to the debit card. If the remote communicator outputs the correct key word, the communicator can read and update the content of the authorization value. The debit card will shut down if the incorrect key word is output four times. After the debit card has recognized the correct key word from the remote communicator, the user of the remote communicator can provide the debit card with an optional updated custom protection word and a corresponding key word for continued use by that customer's particular remote communicator.

In the event that a counterfeit remote communicator is developed where the counterfeit unit contains changes to the original software burnt in the micro processor, protection similar to that used by cellular telephone services can be used.

Although specific embodiments have been illustrated and described herein, it will be appreciated by those of ordinary skill in the art that any arrangement which is calculated to achieve the same purpose may be substituted for the specific embodiment shown. This application is intended to cover any adaptations or variations of the present invention.

CLAIMS

1. A method of authorizing transmissions from a plurality of remote communicators to a base station, the method comprising the steps of:

reading a coded protection word stored on a storage medium of a debit card with one of the plurality of remote communicators;

decoding the coded protection word with one of the plurality of remote communicators and generating a key word based on the decoded protection word;

communicating the key word to the debit card; and

evaluating the key word with the debit card and authorizing the one of the plurality of remote communicators to transmit to the base station based on the key word and an authorization value stored on the storage medium.

2. The method of claim 1 further includes the step of providing the debit card with a custom protection word and a custom key word for use by one of the plurality of remote communicators.

3. The method of claim 1 wherein the authorization value is a pre-determined time value debited accordingly as the one of the plurality of remote communicators transmits to the base station.

4. The method of claim 1 wherein the storage medium is a microprocessor.

5. A method of authorizing transmissions from a plurality of remote communicators to a base station, the method comprising the steps of;

reading a coded protection word stored on a storage medium of a debit card with one of the plurality of remote communicators;

transmitting the coded protection word to the base station using the one of the plurality of remote communicators;

comparing the received coded protection word with a master list of valid coded protection words stored at the base station;

transmitting a validation signal to the one of the plurality of remote communicators indicating if the coded protection word is valid; and

authorizing the one of the plurality of remote communicators to transmit to the base station based on the validation signal and an authorization value stored on the storage medium of the debit card.

6. The method of claim 5 further includes the step of storing a new protection word on the debit card.

7. The method of claim 5 wherein the authorization value is a pre-determined time value debited accordingly as the one of the plurality of remote communicators transmits to the base station.

8. The method of claim 5 wherein the storage medium is a magnetic strip.

9. A method of authorizing transmissions from a plurality of remote communicators to a base station, the method comprising the steps of;

generating a pseudo random code word using one of the plurality of remote communicators;

communicating the pseudo random code word to a debit card comprising a storage medium containing an authorization value and a decoding algorithm;

decoding the pseudo random code word using the decoding algorithm and communicating the decoded pseudo random code word to the one of the plurality of remote communicator; and

reading the authorization value from the storage medium if the decoded pseudo random code word is correct.

10. The method of claim 9 wherein the storage medium is a microprocessor.

11. A remote communication system for two-way messaging with a base station. the remote communication system comprising:

a debit card having a storage medium for storing a coded protection word and an authorization value;

a remote communicator for reading from the storage medium and writing to the storage medium;

a decoder located at the remote communicator for decoding the protection code word read from the storage medium and generating a key word communicated to the debit card; and

an evaluator located at the debit card for evaluating the key word and authorizing the remote communicator to communicate with the base station.

12. The system of claim 11 wherein the storage medium is a microprocessor.

13. A remote communication system for two-way messaging with a base station. the remote communication system comprising:

a debit card having a storage medium for storing a coded protection word and an authorization value;

a remote communicator for reading from the storage medium and writing to the storage medium;

a transmitter located at the remote communicator for transmitting to the base station the coded protection word read from the storage medium; and

a receiver located at the remote communicator for receiving a validation signal indicating the validity of the coded protection word from the base station.

14. The system of claim 13 wherein the storage medium is a magnetic strip.

15. A remote communication apparatus for two-way messaging with a base station for use with a debit card having a storage medium for storing a coded protection word and an authorization value, the remote communication system comprising:

a remote communicator for reading from the storage medium and writing to the storage medium;

a code generator located at the remote communicator for generating a pseudo random code word and communicating the pseudo random code word to the debit card; and

a decoder located at the debit card for decoding the pseudo random code word and communicating the decoded pseudo random code word to the remote communicator, such that the debit card reads the authorization value from the storage medium based on the decoded pseudo random code word.

16. The apparatus of claim 15 wherein the storage medium is a microprocessor.

Fig. 1

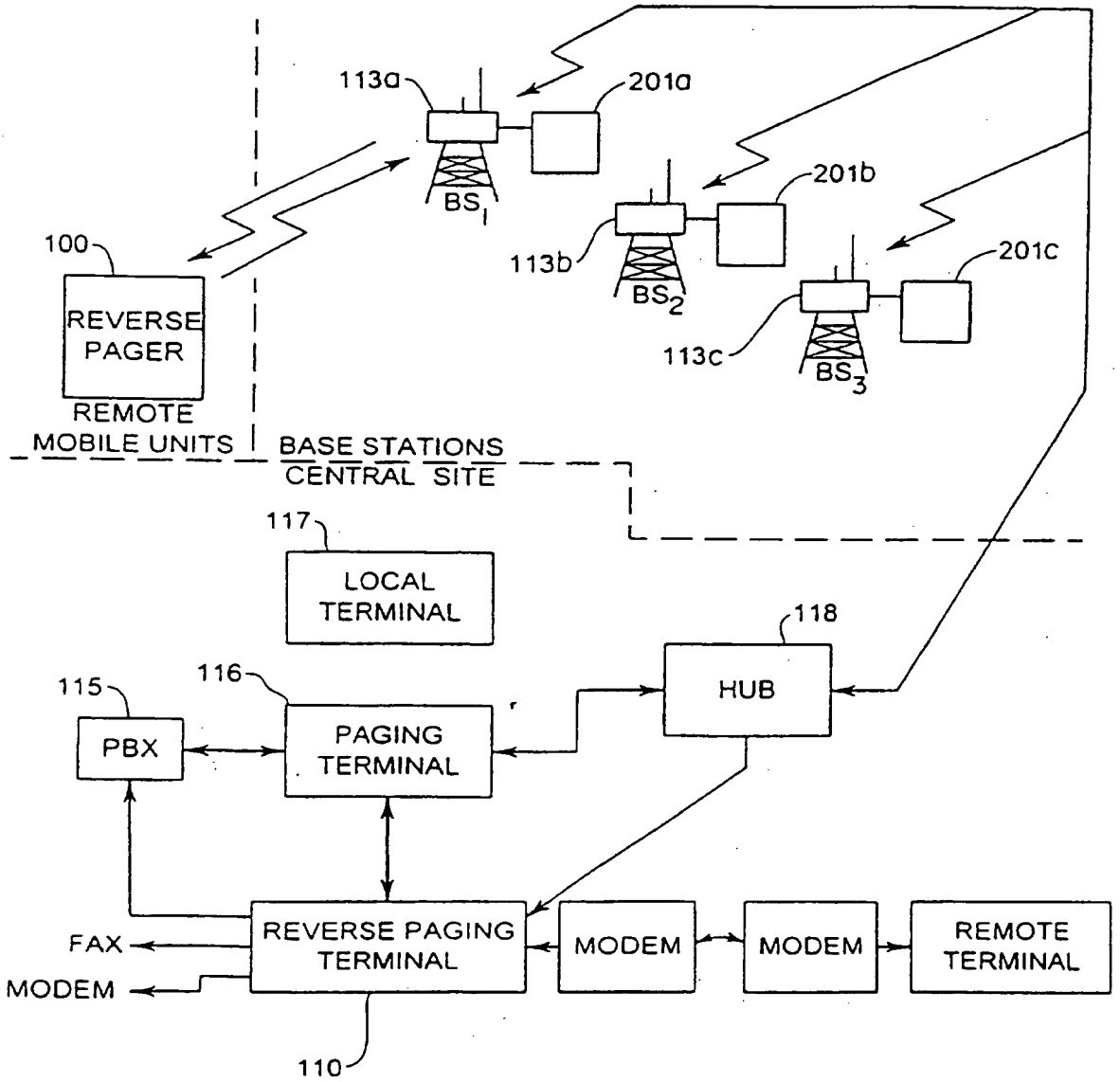

113a
201a
BS1
201b
113b
BS2
201c
113c
BS3
100
REVERSE PAGER
REMOTE MOBILE UNITS
BASE STATIONS CENTRAL SITE
117
LOCAL TERMINAL
118
HUB
115
PBX
116
PAGING TERMINAL
FAX
MODEM
REVERSE PAGING TERMINAL
MODEM
MODEM
REMOTE TERMINAL
110

Fig. 2

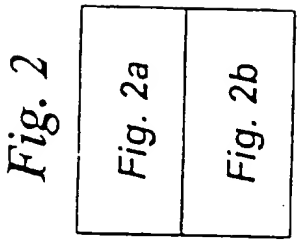


Fig. 2a

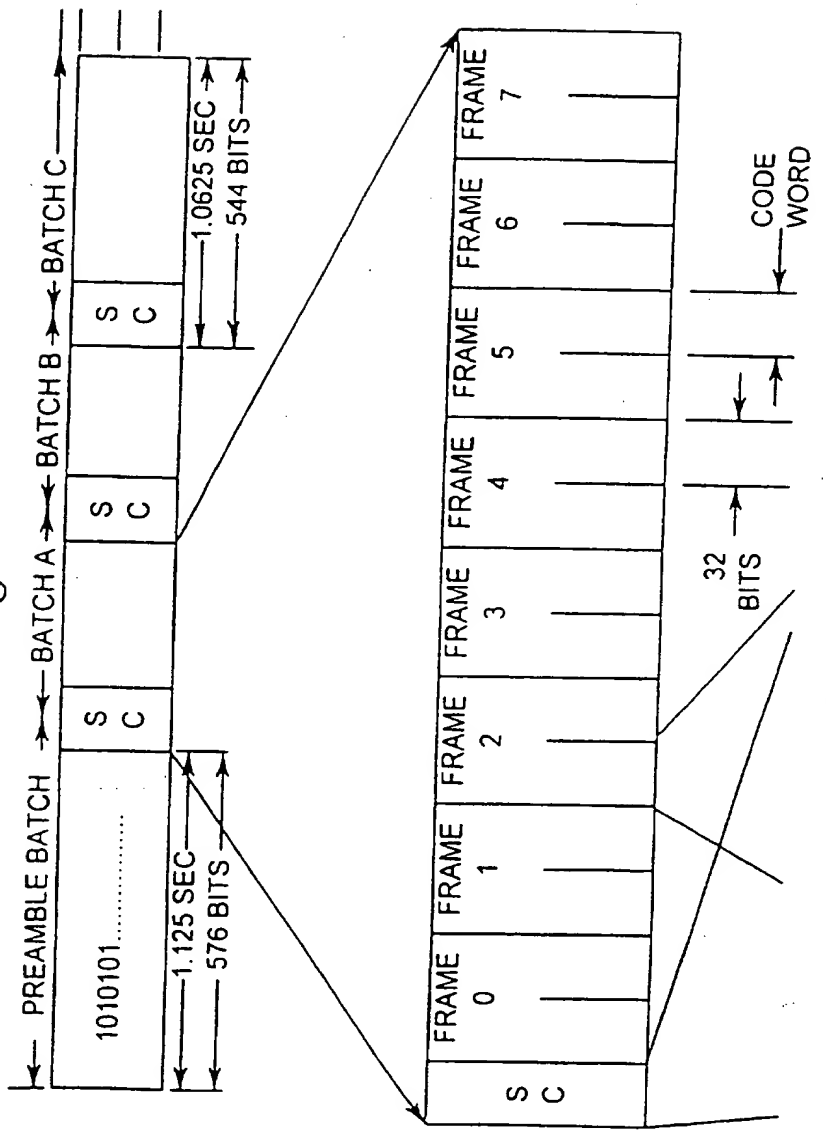
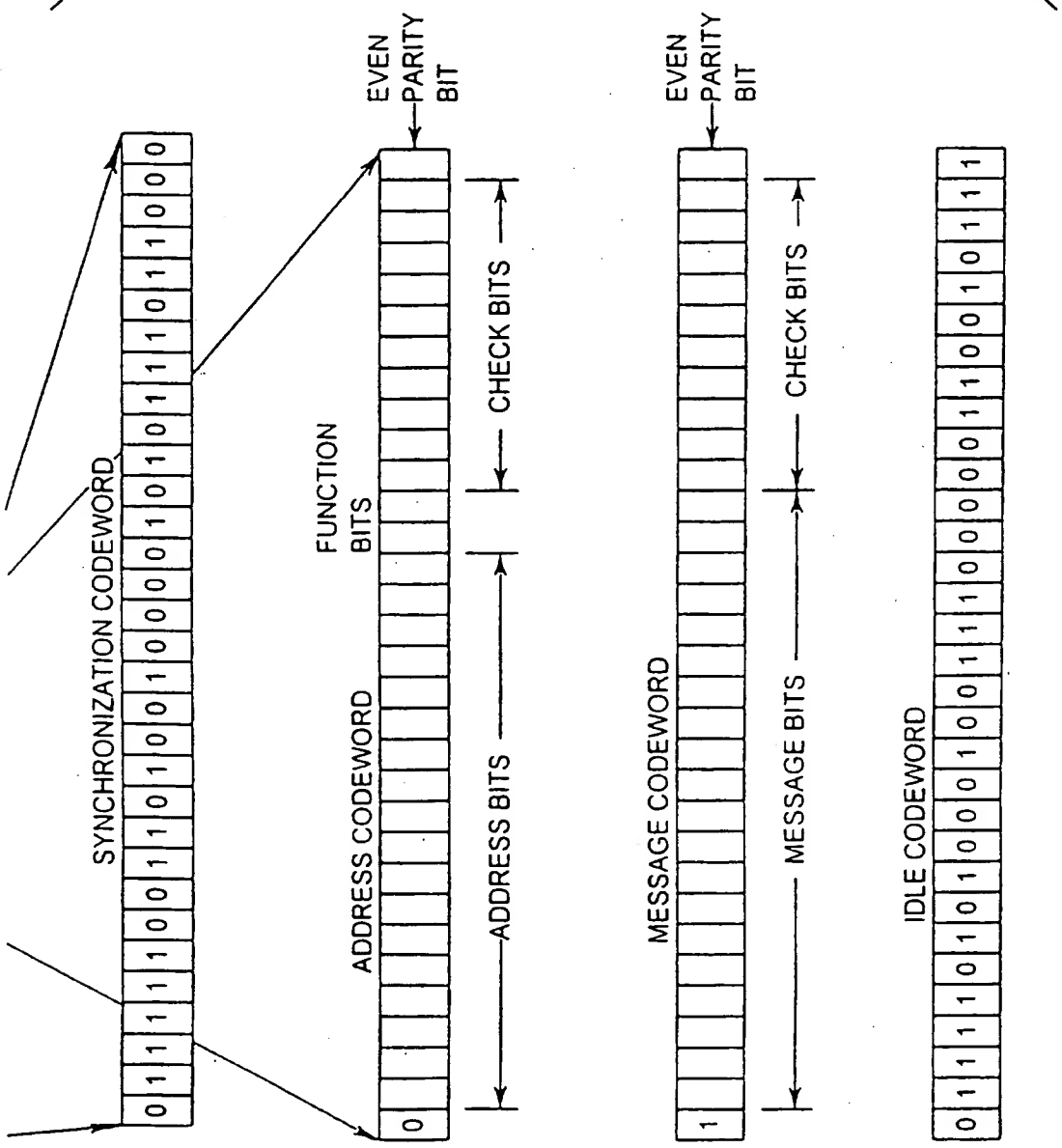


Fig. 2b



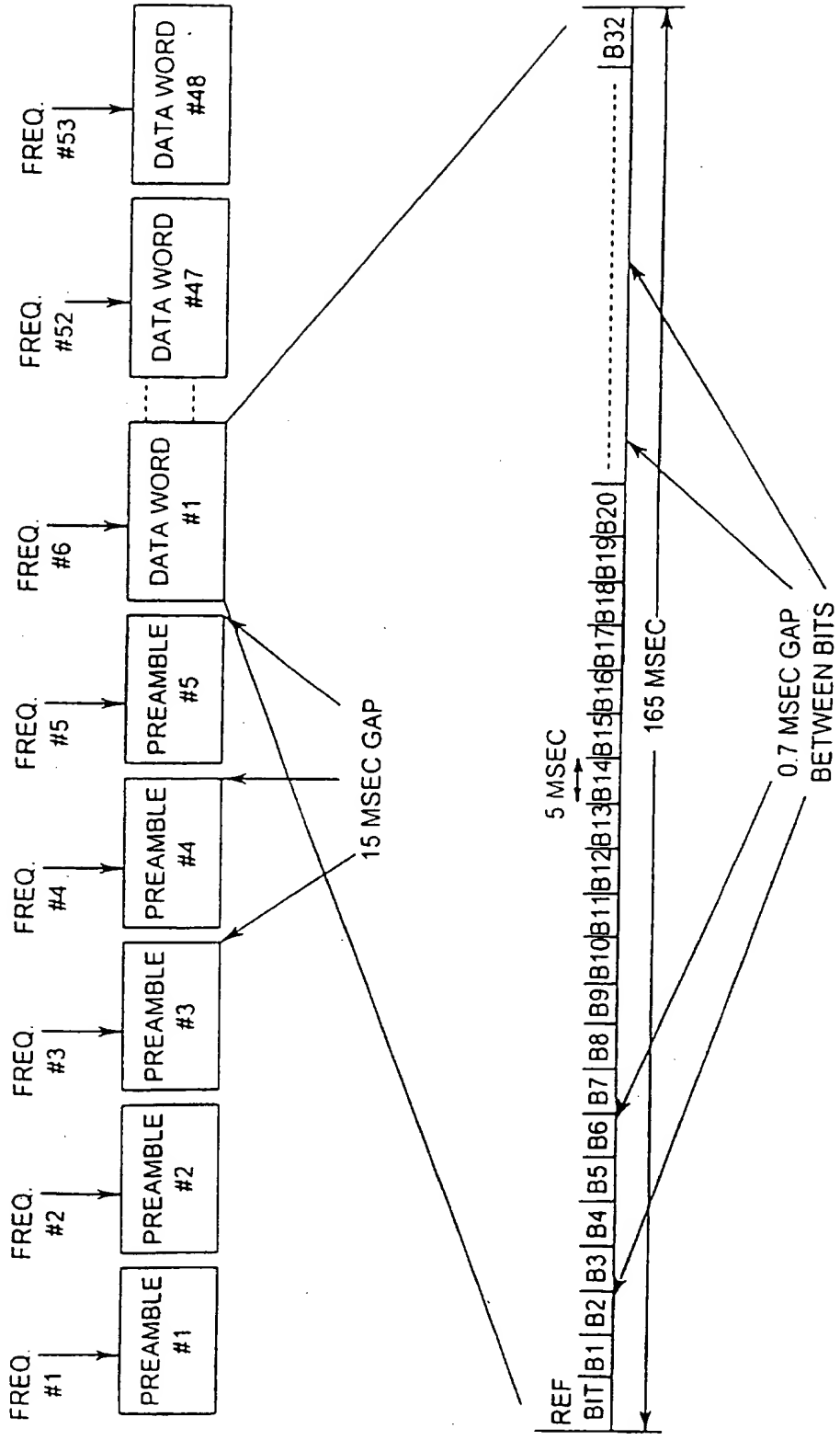


Fig. 3

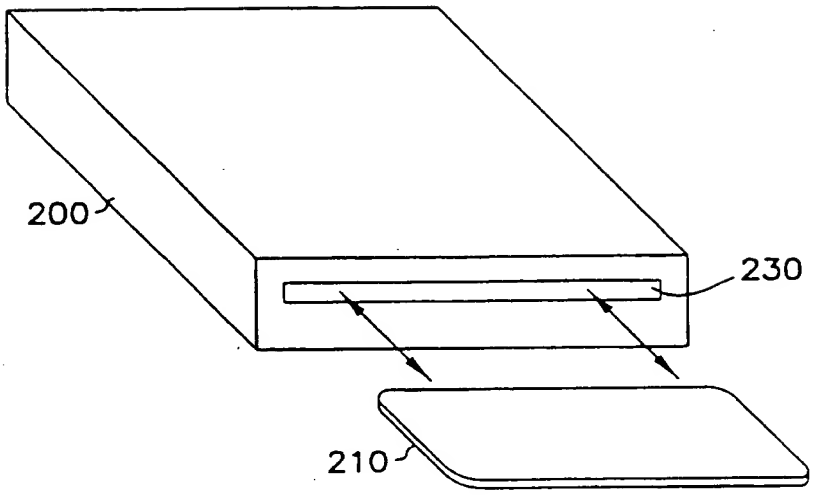


FIG. 4

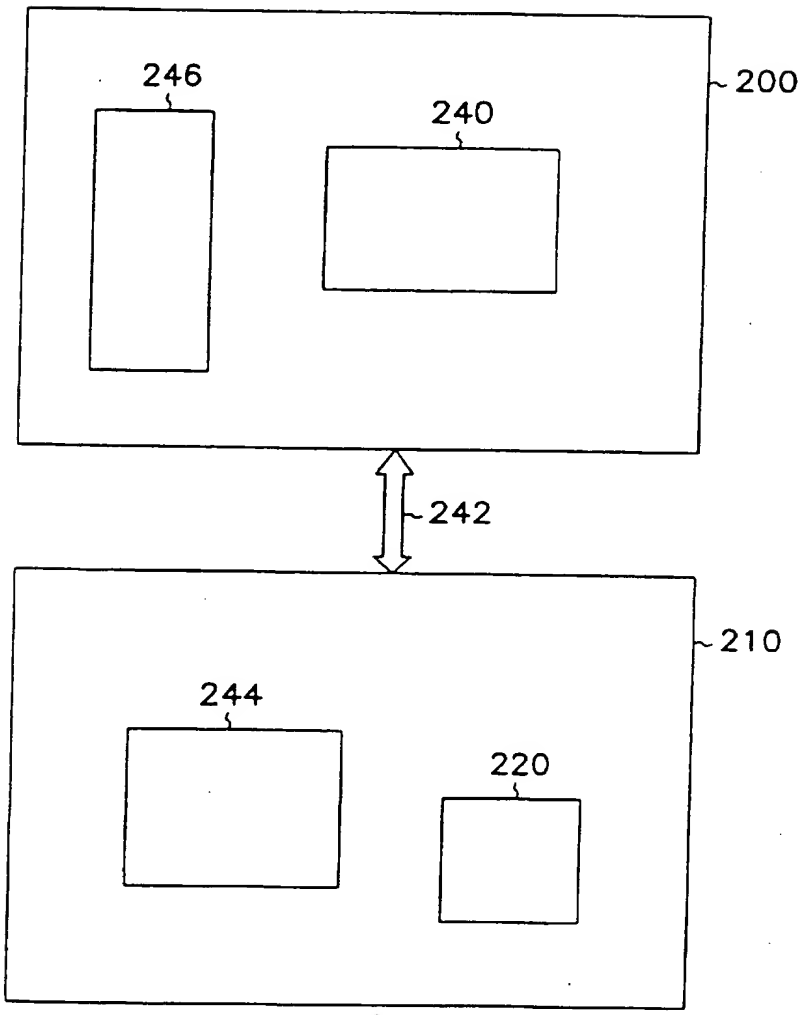


FIG. 5

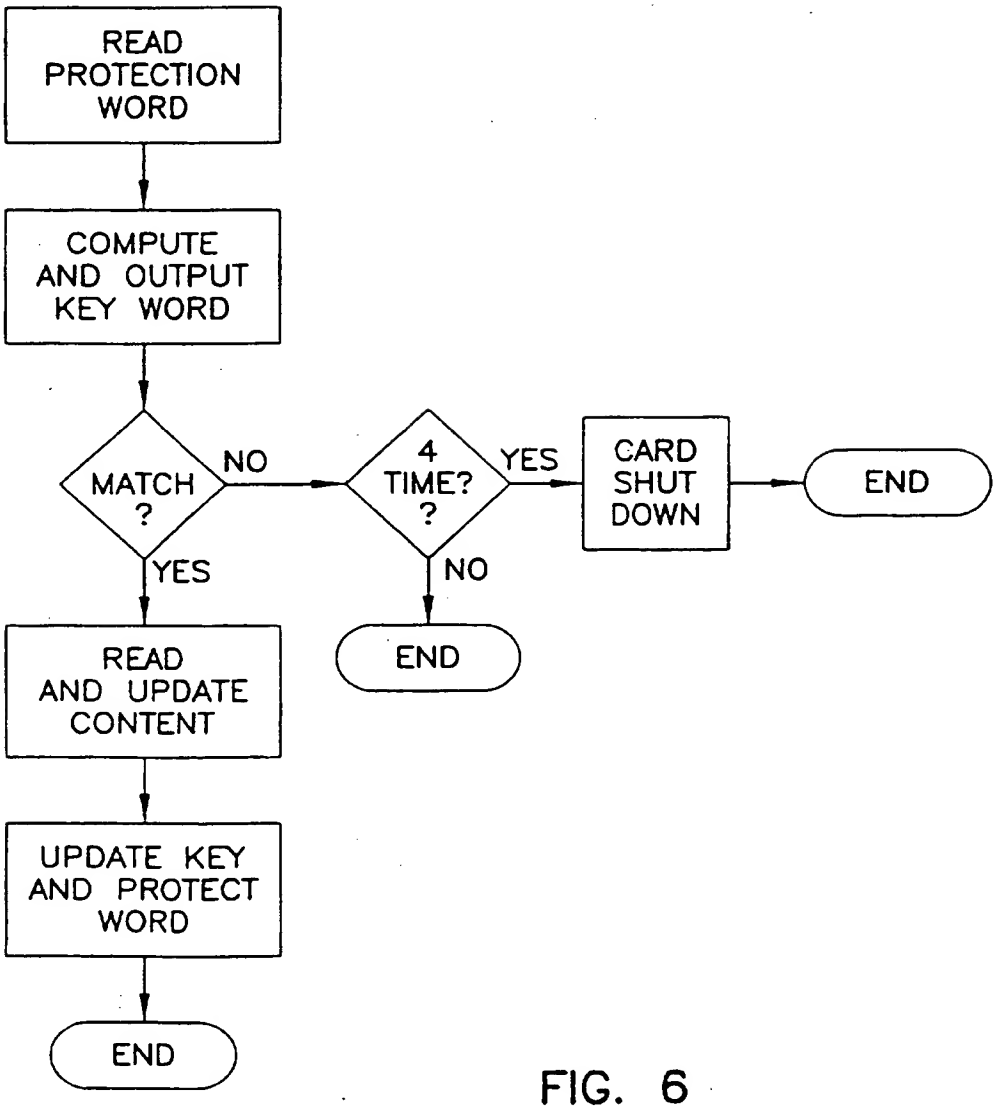

READ PROTECTION WORD
COMPUTE AND OUTPUT KEY WORD
MATCH ?
NO
4 TIME? ?
YES
CARD SHUT DOWN
END
YES
NO
READ AND UPDATE CONTENT
END
UPDATE KEY AND PROTECT WORD
END

FIG. 6

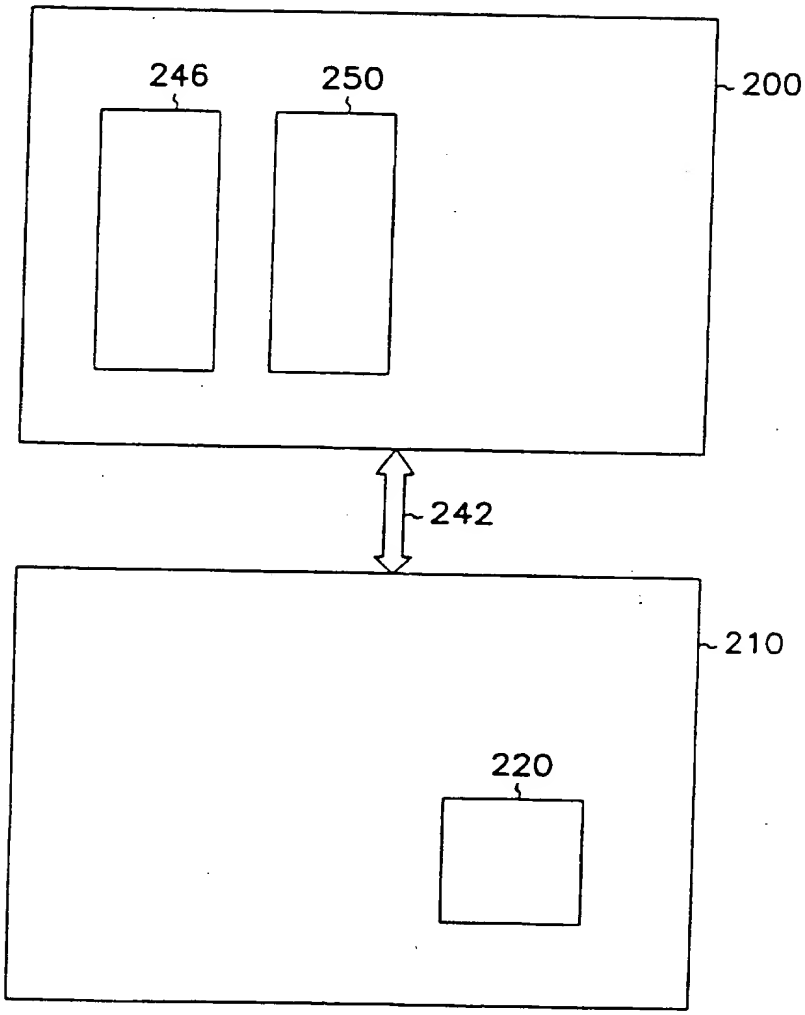


FIG. 7

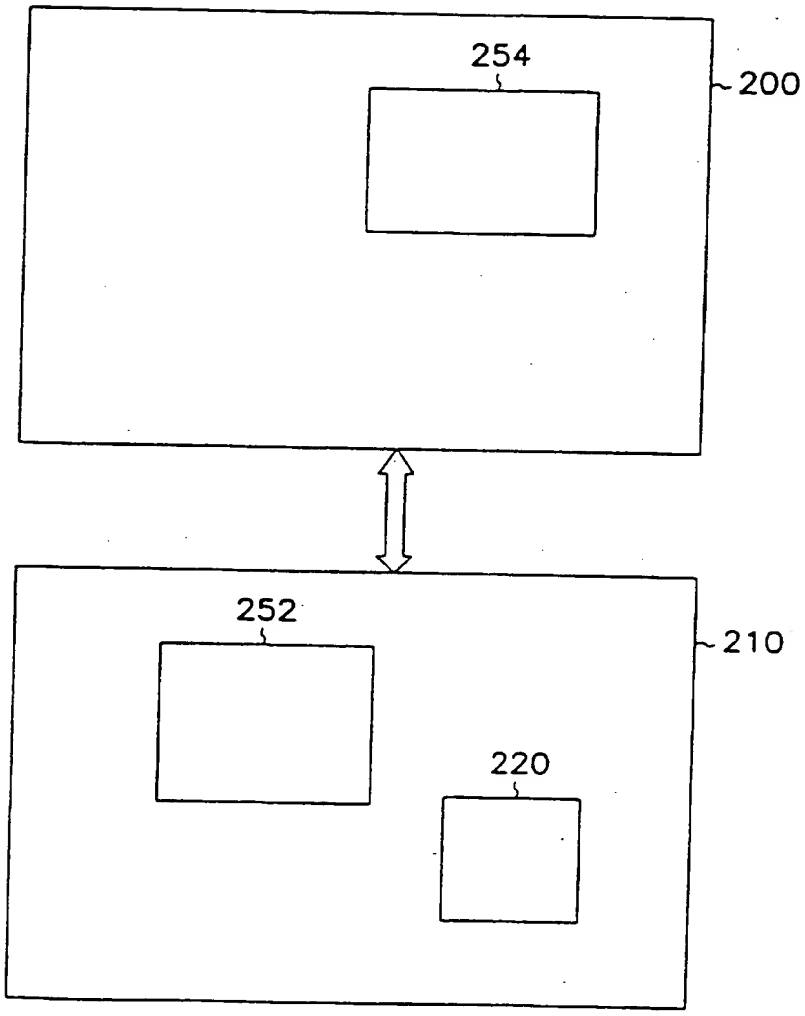


FIG. 8

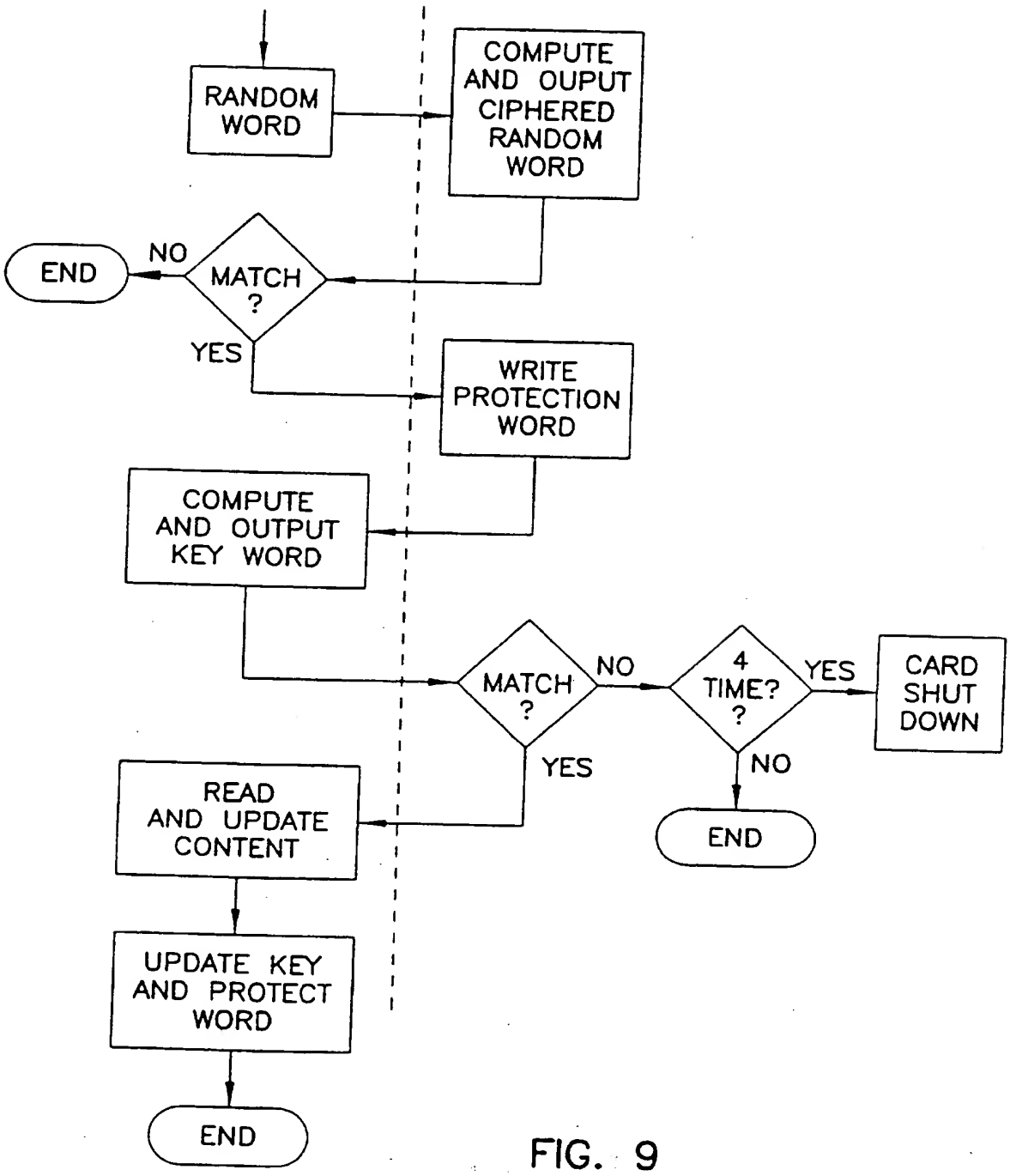


FIG. 9

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/12, H04M 17/00 — A3

(11) International Publication Number: WO 96/24913

(43) International Publication Date: 15 August 1996 (15.08.96)

(21) International Application Number: PCT/GB96/00269

(22) International Filing Date: 6 February 1996 (06.02.96)

(30) Priority Data:
08/386,146 8 February 1995 (08.02.95) US

(71) Applicant: NEXUS 1994 LIMITED [GB/GB]; 7-10 Chandos Street, London W1M 9DE (GB).

(72) Inventors: YOKEV, Hanoch; 8 Hazanchanim Avenue, 52341 Ramat-Gan (IL). MEIMAN, Yehouda; 31 Ben Eliezer Street, 75299 Rishon Letzian (IL).

(74) Agents: BERESFORD, Keith, Denis, Lewis et al.; Beresford & Co., 2-5 Warwick Court, High Holborn, London WC1R 5DJ (GB).

(81) Designated States: JP, KR, SG, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

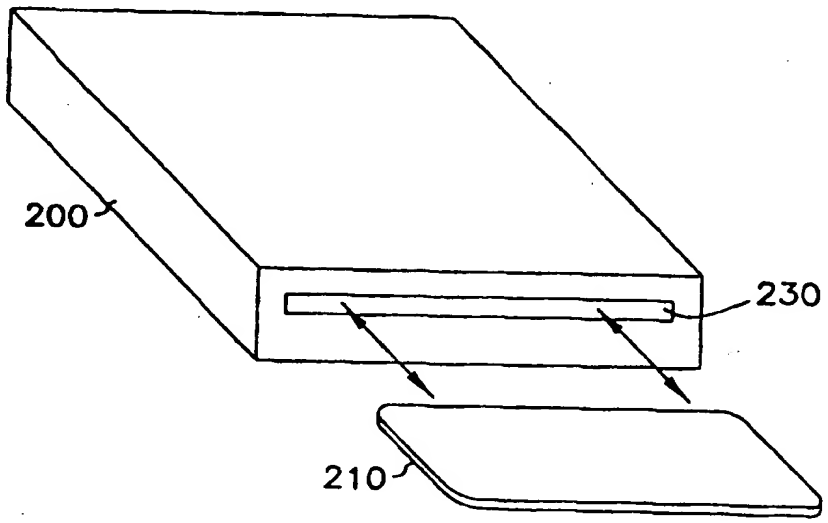
Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(88) Date of publication of the international search report: 26 September 1996 (26.09.96)

(54) Title: TWO-WAY MESSAGING NETWORK USING DEBIT CARDS

(57) Abstract

A two-way messaging network is described which allows a user of a remote communicator to use pre-paid debit cards to authorize message communication. The debit card consists of a storage medium for storing a pre-paid authorization value and anti-counterfeit protection. The remote communicator has the ability to communicate with a base station and debit the authorization value according to the amount of communication time used. The remote communicator also has anti-counterfeiting protection which is used in combination with the debit card to deter unauthorized communications using counterfeit components.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia
AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

INTERNATIONAL SEARCH REPORT

[redacted] onal Application No
[redacted] CT/GB 96/00269

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/12 H04M17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F H04M G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US,A,5 359 182 (D.L. SCHILLING) 25 October 1994 see abstract; claims; figures 1-13 see column 2, line 59 - column 3, line 36 see column 14, line 8 - column 16, line 11 ---	1-16
Y	EP,A,0 216 298 (CASIO COMPUTER) 1 April 1987 see abstract; claims; figure 4 see column 5, line 8 - column 6, line 43 ---	1,2,4, 11,12
Y	EP,A,0 397 512 (MATERIAL ENGINEERING TECHNOLOGY LABORATORY) 14 November 1990 see abstract; claims; figures ---	5,6,8, 13,14
Y	EP,A,0 570 924 (SIEMENS) 24 November 1993 see abstract; claims; figure --- -/--	3,7,9, 10,15,16

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
10 July 1996	26. 07. 96
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	**Authorized officer** David, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 96/00269

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR,A,2 600 188 (BULL CP8) 18 December 1987 ---	
A	FR,A,2 534 712 (TRAITEMENT DE L'INFORMATION) 20 April 1984 ---	
A	EP,A,0 574 990 (PHILIPS ELECTRONICS) 22 December 1993 ---	
A	EP,A,0 589 757 (FRANCE TELECOM) 30 March 1994 ---	
A	EP,A,0 572 991 (S. FROMER) 8 December 1993 -----	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

[redacted]ation on patent family members

[redacted]nal Application No
PCT/GB 96/00269

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
US-A-5359182	25-10-94	CA-A-	2107865	07-04-94
EP-A-0216298	01-04-87	JP-B-	7062862	05-07-95
		JP-A-	62065168	24-03-87
		US-A-	4746788	24-05-88
EP-A-0397512	14-11-90	JP-A-	2297297	07-12-90
EP-A-0570924	24-11-93	EP-A-	0570828	24-11-93
FR-A-2600188	18-12-87	NONE		
FR-A-2534712	20-04-84	NONE		
EP-A-0574990	22-12-93	DE-A-	4219739	23-12-93
		JP-A-	6215208	05-08-94
		US-A-	5436971	25-07-95
EP-A-0589757	30-03-94	FR-A-	2696067	25-03-94
		JP-A-	6268777	22-09-94
		US-A-	5412726	02-05-95
EP-A-0572991	08-12-93	NONE		